# REMARKS

In this response to the above-identified Office Action, Applicants respectfully request reconsideration in view of the above amendments and following remarks. Claims 1 and 8 have been amended. No claims have been added or cancelled. Accordingly, claims 1-4 and 8-16 are pending in the application.

## Claim Amendments

Applicants have **amended claims 1 and 8** to include:

> a braid group $B_n(l)$ divided into a left subgroup $LB_m(l)$ and a right subgroup $RB_{n-l-m}(l)$

(emphasis added). Support for this amendment may be found at least at the top of p. 9 of the specification, or U.S. Pub. No. 2007/0104322, at ¶¶ 0060, lines 1-6.

Applicants have further amended claims 1 and 8 to clarify the claim language. The language:

> an integer $n$ for a number of generators in the braid group $\underline{B_n(l)}$, an integer $m$ for a number of generators in a left subgroup $\underline{LB_m(l)}$, an integer $l$ for an upper bound of a length of a braid

(emphasis added) has been amended to include the braid group and left subgroup designations. The language:

> selecting three braids $x \in LB_m(l), x' \in B_n(l), a \in B_n(l)$

in step 1 has been amended to:

> selecting a braid $x$ generated from the left subgroup $LB_m(l)$, a second braid $x'$ generated from the braid group $B_n(l)$, and a third braid $a$ generated from the braid group $B_n(l)$.

These and other minor amendments have been made in light of clarifying the corresponding technical features, and do not alter the scope of the claim limitations.

Applicants respectfully submit that no new matter has been added, and that the amendments are within the scope of Examiner's search.

**Claims Rejected Under 35 U.S.C. § 102**

Claims 1-4, 13, and 14 stand rejected under 35 U.S.C. § 102(b) as being anticipated by K.H. Ko et al., "New Signature Scheme Using Conjugacy Problem," Nov. 11, 2002, pages 11-13 (hereinafter "Ko"). Applicants respectfully disagree for the following reasons.

To anticipate a claim, a single reference must disclose each element of that claim.

**Claim 1** defines a digital signature scheme based on braid group conjugacy. As amended, claim 1 includes:

> a braid group $B_n(l)$ divided into a left subgroup $LB_m(l)$and a right subgroup $RB_{n-l-m}(l)$

(emphasis added) so as to explicitly distinguish the claim language from Ko. Applicants respectfully submit that this amendment overcomes Examiner's objection that Applicants' previous arguments filed on Oct. 23, 2007 failed to comply with 37 CFR 1.111(b). Office Action, p. 3. Claim 1 also includes in step 3:

> generating braid *b* from the right subgroup $RB_{n-1-m}(l)$ at random.

In contrast to the digital signature method required by the above elements of claim 1, the digital signature method disclosed in Ko does not involve any concept of dividing the braid group "into a left subgroup . . . and a right subgroup," and the random braid *b* is generated within the whole braid group, as opposed to "from the right subgroup." *See* Ko, § 2.3. Ko's method is also described in the Background section of the present application. *See* Specification, at pp. 2-3; or U.S. Pub. No. 2007/0104322, at ¶¶ 0003-0016.

The digital signature scheme disclosed in the application makes use of the exchangeability of a left subgroup and a right subgroup from a divided braid group, and generates a random braid from a subgroup of the braid group. Specification, at p. 6; or U.S. Pub. No. 2007/0104322, at ¶ 0049. Unlike the digital signature method disclosed in Ko, this method reduces the number of the participant braids and the time for conjugacy judgments, overcomes the problems of excessive consumption of computer calculation resources, excessive time for generating key and verifying signature, and greatly improves the signature calculation efficiency without reducing security. Specification, at pp. 6-8; or U.S. Pub. No. 2007/0104322, at ¶¶ 0049-0051.

Thus, Ko does not teach each of the elements of claim 1. Accordingly, reconsideration and withdrawal of the anticipation rejection of this claim are requested.

**Claims 2-4, 13, and 14** depend from independent claim 1, and incorporate the limitations thereof. Thus, at least for the reasons mentioned above in regard to independent claim 1, these claims are not anticipated by Ko. Accordingly, reconsideration and withdrawal of the anticipation rejection of these claims are requested.

## Claims Rejected Under 35 U.S.C. § 103

Claims 1-6, 8-12, and 14-15 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Ko, or in the alternative, under 35 U.S.C. § 103(a) as being obvious over Ko. Applicants respectfully disagree for the following reasons.

To establish a prima facie case of obviousness, the Examiner must show that the cited references, combined, teach or suggest each of the elements of a claim. See In re Vaeck, 947 F.2d 488, 20 USPQ.2d 1438 (Fed. Cir. 1991). Further, the combination of elements must be more than the predictable use of prior art elements according to their established functions. See KSR International Co. v. Teleflex Inc., 550 U.S. ___, 127 S. Ct. 1727 (2007).

Regarding the § 102(b) rejection, independent **claim 8**, as amended, includes elements similar to those of amended claim 1. Thus, at least for the reasons mentioned above in regard to independent claim 1, Ko does not teach each of the elements of claim 8. Accordingly, reconsideration and withdrawal of the anticipation rejection of this claim are requested.

Regarding the § 103(a) rejection, Examiner has not cited and Applicants have not found any reference, such that its combination with Ko teaches or suggests each of the elements of the claim. Further, Examiner has not provided any motivation on which to base any such combination. Thus, Ko does not teach or suggest each of the elements of this claim. Accordingly, reconsideration and withdrawal of the obviousness rejection of this claim are requested.

**Claims 9-12, 15, and 16** depend from independent claim 8, and incorporate the limitations thereof. Thus, at least for the reasons mentioned above in regard to the independent claim, the dependent claims are neither anticipated by nor obvious over Ko. Accordingly, reconsideration and withdrawal of the anticipation and obviousness rejections of these claims are requested.

Applicants believe that all pending claims are allowable and respectfully requests a Notice of Allowance for this application from the Examiner. Should the Examiner believe that a telephone conference would expedite the prosecution of this application; the undersigned can be reached at the telephone number set out below.

The Commissioner is hereby authorized to charge any additional fees due or credit any overpayment to Deposit Account No. 50-2421.

Sincerely,

Dated: March 17, 2008

_/David R. Stevens/_____
David R. Stevens
Reg. No. 38,626

Stevens Law Group
1754 Technology Drive, Suite 226
San Jose, CA 95110
Phone (408) 288-7588
Fax (408) 288-7542